

Robocall Mitigation Plan

Business Information

MCC Network Services, LLC
8 S Washington St.
Suite 200
Sullivan, IL 61951

Contact Information

Kevin Edwards
Voice Network Manager
217-728-9056
support@metrocomm.com

Introduction

MCC Network Services, LLC (“MCC Network”) is a small VSP dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network. MCC Network acquired certain Illinois-market voice service assets. MCC Network now operates under Operating Company Numbers (“OCNs”) 938H, 101J, 9915, and 075A.

MCC Network performs the following roles in the call chain:

- A voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- Our downstream carrier is Inteliquent/Onvoy/Sinch (RMD0003833)

As certified in the FCC’s Robocall Mitigation Database, MCC Network has fully implemented STIR/SHAKEN. TransUnion issues our Certificate with our OCNs.

MCC Network d/b/a Metro Comm and Conxxus, nor any of our executives or principals, have a history of enforcement actions for illegal robocalls, TCPA or TSR violations or related state law violations.

MCC Network has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.

Know Your Customer (“KYC”)

New MCC Network subscribers must provide the following information/documentation:

- name;
- address;
- phone numbers;
- letter of agency/authority;
- billing information from previous carrier;
- signed sales agreement (for business or enterprise customers only).

New subscribers placing outbound calls can only use Caller IDs which have been purchased through our platform or ones validated through automated-number-validation voice call. Pay-by-

invoice is allowed only for subscribers who we know well, with human contact via phone call or in-person at the very least, and credit and associated checks having taken place.

Human contact via phone call or in-person is required in order for new subscribers to gain access to the MCC Network platform (“platform”) to make outbound calls. A subscriber must provide payment through one of the following methods:

- by phone, calling our toll-free number.
- by check via mail.
- online via our payment site.
- through autopay by filling out our ACH form and providing the required information.

MCC Network verifies that each customer’s Emergency 911 address locations are authenticated with the right to present the associated telephone number / Caller ID. Finally, we know our customers personally and understand their use cases.

Know Your Upstream Providers

In accordance with the Commission’s directive in Advanced Methods to Target and Eliminate Unlawful Robocalls, and Call Authentication Trust Anchor, Seventh Report and Order in CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking in CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59, 38 FCC Rcd 5404 (2023), at ¶¶ 49-51, MCC Network provides the following information concerning its upstream voice service carrier.

MCC Network has one upstream provider from which it receives voice traffic:

Inteliquent, Inc. DBA Onvoy, Sinch
1 N Wacker Dr.
Ste 2500
Chicago, IL 60606-2825

MCC Network has a master service agreement with its upstream provider and has received assurances in writing from its officials that it has, and will continue to, sign calls transmitted to MCC Network and will abide by the Commission’s STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to MCC Network. MCC Network and its upstream provider have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy (“AUP”)

MCC Network maintains an AUP that subscribers must agree to before being permitted to use MCC Network’s software and services. In addition, we have implemented a Call Abuse Policy and have incorporated the following policy to our web site’s Acceptable Use Policy (AUP), our terms of use, and have notified our customers of the policy as copied below:

“Any call originated on [MCC Network’s] network is subject to inspection and investigation if the call is suspected of being fraudulent, abusive, or illegal. Calls meeting any of these criteria will be blocked. If these conditions are repeated, becoming excessive, the subscriber may be disconnected from the company’s network, may be subject to further investigation by the FCC for enforcement of the TRACED Act and the subscriber may be subject to fines and penalties imposed by the FCC or the jurisdictional court.”

MCC Network's Terms and Conditions and AUP prohibit use of its services for any purpose other than the intended purpose, including use for criminal activity or use in a manner inconsistent with applicable laws, rules, and regulations, and define the circumstances under which MCC Network will deny, suspend, or terminate services to a customer.

Telephone Number Authorization

New subscribers placing outbound calls can only use Caller IDs which have been purchased through our platform or ones verified through automated-number-validation voice call.

Analytics for Monitoring Traffic

MCC Network works to detect calling patterns consistent with illegal robocalls. If such a call is detected, we will identify the party who is using our network to originate those calls and will take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls on our network.

MCC Network uses the following third-party systems for deploying MCC Network's analytics:

- TNS Call Guardian Authentication Hub (Transaction Network Services) — a fully managed, end-to-end call authentication and robocall analytics solution monitoring originating network traffic for suspicious or abnormal call volume or activity. Call Guardian identifies patterns of suspected illegal robocalls based on behavior and on their status as suspected robocalls as reported to the FCC and Federal Trade Commission and as reported by other carriers, and provides real-time reputation scoring. MCC Network routinely reviews the Call Guardian analytics and takes appropriate action based on the reputation scoring and analytics, in accordance with MCC Network's Terms and Conditions and Acceptable Use Policy.
- Metaview Explorer — monitoring of voice traffic on the Metaswitch platform, specifically SIP floods, multiple calls, and any other suspicious activity.

MCC Network periodically and randomly audits customer equipment. Moreover, MCC Network consults with a firm specializing in Metaswitch in mitigating illegal robocalls.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, MCC Network's risk prevention team is alerted, which follows the defined procedures on investigating such subscribers.

The procedures established include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his or her particular use case and validate that the activity belongs to that subscriber.

MCC Network follows Industry Traceback Group (“ITG”)-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, MCC Network will devote sufficient resources to provide prompt and complete responses to traceback requests. MCC Network commits to responding to traceback requests fully within 24 hours.

MCC Network will promptly respond to Do Not Originate requests it receives from ITG. In addition, our carrier, Inteliquent, also conforms to Do Not Originate requests and protocols. MCC Network has mechanisms to automatically block suspicious calls using internal analytics.

If MCC Network’s monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, MCC Network will take appropriate action which may include suspending or terminating the subscriber’s use of MCC Network’s network. MCC Network will cooperate with investigative bodies (provide a single point of contact to address traceback requests from law enforcement including state attorneys general offices), to the FCC, and/or ITG; as well as documenting requests and actions taken in response thereto.

Plan Updates

This plan, along with industry best practices, will evolve to respond to the dynamic nature of mitigating illegal robocalling. MCC Network will monitor industry best practices and continuously improve our internal processes to ensure this plan, and our system adapts to this ever-changing issue. In the event of any material change to this plan, MCC Network will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) business days of such update.